



[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

SEARCH

THE ACM DIGITAL LIBRARY

[Feedback](#)

("intrusion detection system" and probe and packet)

Terms used: **intrusion detection**

**system probe packet**

Found 80 of 244,119

Sort results by

relevance

Display results

expanded form



Save

results

to a

[Binder](#)

☐ Open results in a new window

Refine these results with

[Advanced](#)

[Search](#)

Try this search in [The](#)

[ACM](#)

[Guide](#)

Results 1 - 20 of 80 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [next](#)

>>>

# [1 Measuring intrusion detection capability: an information-theoretic approach](#)



Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee, Boris Skori\*

March 2006 ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security

**Publisher:** ACM

Full text available: [pdf\(381.84 KB\)](#)

[KB](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#),


[index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 20, Downloads (12 Months): 328, Citation Count: 1


A fundamental problem in intrusion detection is what metric(s) can be used to objectively evaluate an intrusion detection system (IDS) in terms of its ability to correctly classify events as normal or intrusive. Traditional metrics (e.g., true positive ...

**Keywords:** information-theoretic, intrusion detection, performance measurement

## 2 [Challenging the anomaly detection paradigm: a provocative discussion](#)

 Carrie Gates, Carol Taylor  
September 2006 NSPW '06: Proceedings of the 2006 workshop on New security paradigms

**Publisher:** ACM

Full text available:  [pdf\(145.52 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#)

**Bibliometrics:** Downloads (6 Weeks): 31, Downloads (12 Months): 173, Citation Count: 1


In 1987, Dorothy Denning published the seminal paper on anomaly detection as applied to intrusion detection on a single system. Her paper sparked a new paradigm in intrusion detection research with the notion that malicious behavior could be distinguished ...

**Keywords:** intrusion detection, security

## 3 [Balancing cooperation and risk in intrusion detection](#)

 Deborah Frincke  
February 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 1

**Publisher:** ACM

Full text available:  [pdf\(236.44 KB\)](#)


**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 12, Downloads (12 Months): 131, Citation Count: 6


Early systems for networked intrusion detection (or, more generally, intrusion or misuse management) required either a centralized architecture or a centralized decision-making point, even when the data gathering was distributed. More recently, researchers ...

**Keywords:** access control models, authorization mechanisms, collaborative systems

## 4 [Sensor-based intrusion detection for intra-domain distance-vector routing](#)

 Vishal Mittal, Giovanni Vigna  
November 2002 CCS '02: Proceedings of the 9th ACM conference on Computer and communications security

**Publisher:** ACM

Full text available:  [pdf\(267.99 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#)

**Bibliometrics:** Downloads (6 Weeks): 4, Downloads (12 Months): 76, Citation Count: 3

Detection of routing-based attacks is difficult because malicious routing behavior can be identified only in specific network locations. In addition, the configuration of the signatures used by intrusion detection sensors is a time-consuming and error-prone ...

**Key words:** intrusion detection, network topology, routing security


## 5 Enhancing byte-level network intrusion detection signatures with context



Robin Sommer, Vern Paxson

October      CCS '03: Proceedings of the 10th ACM conference on Computer and communications security

**Publisher:** ACM

Full text available:  [pdf\(217.88 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 17, Downloads (12 Months): 170, Citation Count: 12

Many network intrusion detection systems (NIDS) use byte sequences as signatures to detect malicious activity. While being highly efficient, they tend to suffer from a high false-positive rate. We develop the concept of *contextual signatures* as ...


**Key words:** bro, evaluation, network intrusion detection, pattern matching, security, signatures, snort

## 6 A new intrusion detection system using support vector machines and hierarchical clustering

Latifur Khan, Mamoun Awad, Bhavani Thuraisingham

October      The VLDB Journal — The International Journal on Very Large Data Bases, Volume 16 Issue 4

**Publisher:** Springer-Verlag New York, Inc.

Full text available:  [pdf\(514.93 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 38, Downloads (12 Months): 49, Citation Count: 0

Whenever an intrusion occurs, the security and value of a computer system is compromised. Network-based attacks make it difficult for legitimate users to access various network services by purposely occupying or sabotaging network resources and services. ...

## 7 A framework for constructing features and models for intrusion detection systems



Wenke Lee, Salvatore J. Stolfo

November 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 4

**Publisher:** ACM

Full text available:  [pdf\(187.03 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

**Bibliometrics:** Downloads (6 Weeks): 28, Downloads (12 Months): 491, Citation Count: 30

Intrusion detection (ID) is an important component of infrastructure protection mechanisms. Intrusion detection systems (IDSs) need to be accurate, adaptive, and extensible. Given these requirements and the complexities of today's network environments, ...

**Keywords:** data mining, feature construction, intrusion detection

## 8 Anomalous system call detection



Darren Mutz, Fredrik Valeur, Giovanni Vigna, Christopher Kruegel

February 2006 ACM Transactions on Information and System Security (TISSEC), Volume 9 Issue 1

**Publisher:** ACM

Full text available:  [pdf\(645.58 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 31, Downloads (12 Months): 371, Citation Count: 0

Intrusion detection systems (IDSs) are used to detect traces of malicious activities targeted against the network and its resources. Anomaly-based IDSs build models of the expected behavior of applications by analyzing events that are generated during ...

**Keywords:** Bayesian network, Intrusion detection, anomaly detection, computer security

## 9 TCM-KNN scheme for network anomaly detection using feature-based optimizations



Yang Li, Li Guo

March 2008 SAC '08: Proceedings of the 2008 ACM symposium on Applied computing 2008

**Publisher:** ACM

Full text available:  [pdf\(137.72 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 0, Downloads (12 Months): 0, Citation Count: 0

With the rapid increase of network threats and cyber attacks, network security problem is becoming more and more serious. Network anomaly detection is a key technique to secure information systems and resist cyber attacks. In this paper, we first propose ...

**Keywords:** TCM-KNN algorithm, anomaly detection, feature selection, feature weight, network security

## 10 [Is sampled data sufficient for anomaly detection?](#)



Jianning Mai, Chen-Nee Chuah, Ashwin Sridharan, Tao Ye, Hui Zang

October 2006 IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement

**Publisher:** ACM

Full text available: [pdf\(1.83 MB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index](#)

[terms](#)

**Bibliometrics:** Downloads (6 Weeks): 13, Downloads (12 Months): 149, Citation Count: 1

Sampling techniques are widely used for traffic measurements at high link speed to conserve router resources. Traditionally, sampled traffic data is used for network management tasks such as traffic matrix estimations, but recently it has also been used ...

**Keywords:** anomaly detection, portscan, sampling, volume anomaly

## 11 [Internet intrusions: global characteristics and prevalence](#)



Vinod Yegneswaran, Paul Barford, Johannes Ullrich

June 2003 ACM SIGMETRICS Performance Evaluation Review, Volume 31 Issue 1

**Publisher:** ACM

Full text available: [pdf\(699.44 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#),

[index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 22, Downloads (12 Months): 156, Citation Count: 15

Network intrusions have been a fact of life in the Internet for many years. However, as is the case with many other types of Internet-wide phenomena, gaining insight into the *global* characteristics of intrusions is challenging. In this paper we ...

**Keywords:** internet performance and monitoring, network security, wide area measurement

## 12 [A high-level programming environment for packet trace anonymization and transformation](#)



Ruoming Pang, Vern Paxson

August 2003 SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications

**Publisher:** ACM

Full text available: [pdf\(251.27 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#),

[index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 9, Downloads (12 Months): 66, Citation Count: 14

Packet traces of operational Internet traffic are invaluable to network research, but public sharing of such traces is severely limited by the need to first remove all sensitive information. Current trace anonymization technology leaves only the packet ...

**Keyw ords:** anonymization, internet, measurement, network intrusion detection, packet trace, privacy, transformation

## 13 [Network intrusion detection through Adaptive Sub-Eigenspace Modeling in multiagent systems](#)



Mei-Ling Shyu, Thiago Quirino, Zongxing Xie, Shu-Ching Chen, Liwu Chang

September 2007 ACM Transactions on Autonomous and Adaptive Systems (TAAS), Volume 2 Issue 3

**Publisher:** ACM

Full text available: [pdf\(1.93 MB\)](#)


**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)


**Bibliometrics:** Downloads (6 Weeks): 50, Downloads (12 Months): 543, Citation Count: 0

Recently, network security has become an extremely vital issue that beckons the development of accurate and efficient solutions capable of effectively defending our network systems and the valuable information journeying through them. In this article, ...

**Keyw ords:** Agent communications, adaptive sub-eigenspace modeling (ASEM), agent-based distributed system, intrusion detection, network security

#### 14 [Dendritic cells for SYN scan detection](#)

 Julie Greensmith, Uwe Aickelin  
July GECCO '07: Proceedings of the 9th annual conference on Genetic and  
2007 evolutionary computation  
**Publisher:** ACM

Full text available:  [pdf\(2.87 MB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


**Bibliometrics:** Downloads (6 Weeks): 7, Downloads (12 Months): 119, Citation Count: 0

Artificial immune systems have previously been applied to the problem of intrusion detection. The aim of this research is to develop an intrusion detection system based on the function of Dendritic Cells (DCs). DCs are antigen presenting cells and key ...

**Key words:** artificial immune systems, dendritic cells, port scans

#### 15 [Network anomaly detection based on TCM-KNN algorithm](#)

 Yang Li, Binxing Fang, Li Guo, You Chen  
March ASI ACCS '07: Proceedings of the 2nd ACM symposium on Information,  
2007 computer and communications security  
**Publisher:** ACM

Full text available:  [pdf\(160.77 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


**Bibliometrics:** Downloads (6 Weeks): 22, Downloads (12 Months): 380, Citation Count: 0

Intrusion detection is a critical component of secure information systems. Network anomaly detection has been an active and difficult research topic in the field of Intrusion Detection for many years. However, it still has some problems unresolved. They ...

**Key words:** TCM-KNN algorithm, anomaly detection, machine learning, network security

#### 16 [Learning attack strategies from intrusion alerts](#)

 Peng Ning, Dingbang Xu  
October CCS '03: Proceedings of the 10th ACM conference on Computer and  
2003 communications security  
**Publisher:** ACM

Full text available:  [pdf\(248.17 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#),  
[index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 21, Downloads (12 Months): 201, Citation Count: 5

Understanding strategies of attacks is crucial for security applications such as computer and network forensics, intrusion response, and prevention of future attacks. This paper presents techniques to automatically learn attack strategies from correlated ...

**Key words:** alert correlation, intrusion detection, profiling attack strategies

## 17 Towards NIC-based intrusion detection



M. Otey, S. Parthasarathy, A. Ghoting, G. Li, S. Naravula, D. Panda  
August KDD '03: Proceedings of the ninth ACM SIGKDD international conference on  
2003 Knowledge discovery and data mining

**Publisher:** ACM

Full text available: [pdf\(103.59 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 9, Downloads (12 Months): 98, Citation Count: 1

We present and evaluate a NIC-based network intrusion detection system. Intrusion detection at the NIC makes the system potentially tamper-proof and is naturally extensible to work in a distributed setting. Simple anomaly detection and signature detection ...

**Key words:** NICs, data mining, network interface cards, network intrusion detection, network security

## 18 A formal approach to sensor placement and configuration in a network intrusion detection system



Marco Rolando, Matteo Rossi, Niccolò Sanarico, Dino Mandrioli  
May SESS '06: Proceedings of the 2006 international workshop on Software  
2006 engineering for secure systems

**Publisher:** ACM

Full text available: [pdf\(228.55 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#),  
[index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 24, Downloads (12 Months): 109, Citation Count: 1

Network Intrusion Detection Systems (NIDSs) can be composed of a potentially large number of sensors, which monitor the traffic flowing in the network. Deciding *where* sensors should be placed and *what* information they need in order to detect ...

**Key words:** formal model, intrusion detection systems, network analysis, sensor configuration, sensor placement



## 19 [Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA](#)



### [intrusion detection system evaluations as performed by Lincoln Laboratory](#)

November 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 4

**Publisher:** ACM

Full text available: [pdf\(156.16 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

**Bibliometrics:** Downloads (6 Weeks): 40, Downloads (12 Months): 355, Citation Count: 23

In 1998 and again in 1999, the Lincoln Laboratory of MIT conducted a comparative evaluation of intrusion detection systems (IDSs) developed under DARPA funding. While this evaluation represents a significant and monumental undertaking, there are a number ...

**Keywords:** computer security, intrusion detection, receiver operating curves (ROC), software evaluation

## 20 [Constructing attack scenarios through correlation of intrusion alerts](#)



Peng Ning, Yun Cui, Douglas S. Reeves

November 2002 CCS '02: Proceedings of the 9th ACM conference on Computer and communications security

**Publisher:** ACM

Full text available: [pdf\(184.18 KB\)](#)

**Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 25, Downloads (12 Months): 200, Citation Count: 13

Traditional intrusion detection systems (IDSs) focus on low-level attacks or anomalies, and raise alerts independently, though there may be logical connections between them. In situations where there are intensive intrusions, not only will actual alerts ...

**Keywords:** alert correlation, attack scenarios, intrusion detection

---

Results 1 - 20 of 80 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [next](#)

[>](#) [>>](#)

The ACM Portal is published by the

Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)